Offer Description: Secure Email

This Offer Description (**"Offer Description"**) describes Cisco Secure Email Cloud Gateway (formerly Cloud Email Security or "CES"), Cisco Secure Email Encryption Service (formerly Cisco Registered Envelope Service or "CRES"), Cisco Secure Email Domain Protection (formerly Cisco Domain Protection or "DMP"), Cisco Secure Email Phishing Defense (formerly Cisco Advanced Phishing Protection or "APP") and Cisco Secure Email Cloud Mailbox (formerly Cisco Cloud Mailbox Defense or "CMD") (collectively, the **"Cloud Service(s)"**). Your subscription is governed by this Offer Description and the Cisco End User License Agreement located at http://www.cisco.com/go/eula (or similar terms existing between the parties) (the **"Agreement"**). If capitalized terms are not defined in this Offer Description, then they have the meaning given to them in the Agreement or order(s).

1. Description

1.1. Cisco Secure Email Cloud Gateway and Cisco Secure Email Envelope Encryption

Cisco Secure Email Cloud Gateway is a cloud-based email security service that blocks spam and security threats from the Internet. This product includes the option to license Cisco Secure Email Encryption Service which helps companies secure their email communications by allowing businesses to send encrypted messages via registered envelopes.

1.2. Cisco Secure Email Domain Protection

Cisco Secure Email Domain Protection helps prevent phishing emails from being sent using a customer domain. This product automates the process of implementing the email authentication standard Domain Message Authentication Reporting & Conformance ("**DMARC**") to better protect Your employees, customers and suppliers from phishing attacks using a Your domain. Doing so protects Your brand identity as well as increases email marketing effectiveness by reducing phishing messages from reaching inboxes.

1.3. Cisco Secure Email Phishing Defense

Cisco Secure Email Phishing Defense stops identity deception-based attacks such as social engineering, impostors, and business email compromise. It further provides local email intelligence and advanced machine learning techniques to model trusted email behavior on the Internet, within organizations and between individuals. This product's protection integrates machine learning techniques to drive daily model updates, maintaining a real-time understanding of email behavior to stop identity deception.

1.4. Cisco Secure Email Cloud Mailbox

Cisco Secure Email Cloud Mailbox is a cloud-based email security service that blocks spam and security threats from the Internet. Features include anti-spam, intelligent multi-scan anti-spam, anti-virus, anti-phishing detection and advanced malware protection.

1.5. Cisco SecureX

Your Cisco Secure Email Cloud Gateway and Cisco Secure Email Cloud Mailbox subscriptions include access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence. For more information, please see the SecureX Offer Description at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html.

2. Supplemental Terms and Conditions

2.1. Licensing and Use Limitations

a. The Cloud Services described in this Offer Description are licensed based on the quantity of Covered Users. The term "**Covered Users**" means the total number of your internet-connected employees, subcontractors and other authorized individuals covered by your deployment of the applicable Cloud Service.

b. If we determine in good faith that You are using Cisco Secure Email Cloud Gateway or Cisco Secure Email Cloud Mailbox as part of an outbound bulk email delivery service, Cisco may require You to purchase additional services or require You to re-architect the email flow to exclude one or both of those products from Your outbound bulk email flow.

2.2. Disclaimers

WE DO NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. WE DO NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD-PARTY MALICIOUS ATTACKS. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS.

3. Service Level Agreements

3.1. Definitions

The following defined terms apply to all Service Level Agreements (each an "**SLA**", or collectively, "**SLAs**") found in this Offer Description:

- "**Caught Spam**" means Spam that is either quarantined or categorized as a "threat message" in the user interface.
- "**Emergency Maintenance**" means any time outside of the Scheduled Maintenance Window that We are required to apply urgent patches, fixes, or undertake other urgent maintenance activities.
- "**Infraction**" means a single instance of unavailability in accordance with the specific calculation set forth in each applicable SLA. Separate occurrences cannot be aggregated for purposes of determining whether an Infraction has occurred.
- "**Known Virus**" means a Virus defined solely by the provider of anti-virus software that is used for a specific message or file.
- "**Missed Spam**" is Spam delivered to a Covered User's email inbox.
- "**Scheduled Maintenance Window**" means the window of scheduled maintenance for the applicable Cloud Services.
- "**Service Availability**" means the percentage of total time during which the Cloud Services (including but not limited to the applicable Cloud Services portal) is available to You and operating properly without material degradation, excluding up to 30 minutes per month for Scheduled Maintenance and Emergency Maintenance.
- "**Service Credit(s)**" means the percentage of Calculated Monthly Fees paid that is awarded to You for validated claim(s) resulting from a breach of an applicable SLA or SLAs. The "**Calculated Monthly Fee**" is defined as fees received for Your annual subscription for the Cloud Services divided by 12 months.
- "**Spam**" means unsolicited or unauthorized bulk electronic mail (SMTP only), including marketing messages.
- "**Virus**" means a binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, CPU cycles or network bandwidth on the infected host, use the infected host to

replicate itself to other hosts, or provide control or access to any of the infected host's system resources. A Virus does not include: (1) text messages that use fraudulent claims to deceive You, and/or prompt You to action, (2) a binary or executable code installed or run by a Covered User that gathers information for sales or marketing purposes, (3) a Virus that may be detected and cleaned by other Virus scanning products, or (4) an ineffective or inactive Virus fragment.

3.2. Service Credits and General Exceptions

a. All remedies for breach of an SLA are conditioned upon Your (1) payment of all applicable fees, (2) fulfilling all Your obligations under the Agreement and this Offer Description, and (3) Your submission of a claim in accordance with the SLA Claim Procedure described below. If You have earned Service Credits but have prepaid for a subscription in full and do not renew, then all such earned Service Credits will be forfeited.

b. Service Credits earned will be applied to either (1) the subscription fee for the next subscription term if You have prepaid for the then-current subscription in full, or (2) the next installment payment amount owed if You are paying for the subscription on a monthly, quarterly, or annual installment basis.

c. Service Credits do not apply as a result of the Cloud Services failing to meet a particular SLA due to any of the following (the "**General Exceptions**"):

- Any Infraction caused by Your action or omissions.
- Hardware or software upgrades, facility upgrades, or other similar Customer-led network interruptions;
- A Scheduled Maintenance Window that was announced at least 24 hours in advance;
- Hardware, software or other data center equipment or services not within Our control, or outside the scope of the Cloud Services;
- Hardware or software configuration changes that You made;
- Denial of service attacks on Our infrastructure or ancillary services such as SenderBase; or
- Events outside of Our reasonable control, including acts of God, earthquake, labor disputes, industry wide shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemic, or delays of common carriers.

3.3. Exclusive Remedy and SLA Claim Procedure

a. The Service Credits available to You under the applicable SLAs are Your sole and exclusive remedy for Cisco's failure to meet service levels identified in this Section 3.

b. You must submit a claim for Service Credits within 30 calendar days of the claimed Infraction. Additionally, each claim:

- Must be supported with evidence from message logs, sample messages, support ticket numbers, ping or trace route data, reporting data or other applicable method for documenting the occurrence and duration of the claimed Infraction;
- Must certify that: (1) no changes or actions initiated by You were responsible for the occurrence resulting in the claimed Infraction, and (2) You did not ignore warnings by Cisco of certain behavior that is responsible for such occurrence—including but not limited to: the presence of a mail loop due to configuration within or external to the Cloud Services; creating a policy bypass around anti-spam policies in the policy configuration; creating a policy bypass around anti-virus filtering in the configuration; misconfiguration of an encryption profile; or failure to permit upgrade of the PXE-SDK or any other software version of the Cloud Services; and

- Must be submitted through a support ticket.

c. We will evaluate each claim, respond within 48 hours regarding the validity of such claim, and, if validated, provide You with the applicable Service Credits within 30 days following Our response.

3.4. Cisco Secure Email Cloud Gateway SLAs

a. Uptime SLA: Cisco Secure Email Cloud Gateway will accept connections on Port 25 and process email at least 99.999% of the time during each calendar month, excluding Scheduled Maintenance Windows and Emergency Maintenance ("**Uptime**"). Uptime is determined by dividing the total number of minutes this product was processing email divided by the number of minutes in that calendar month. If You experience an Uptime Infraction, then subject to the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Service Availability	Service Credit as a % of Monthly Fee
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

b. Delivery Time SLA: Cisco Secure Email Cloud Gateway will process email messages so that the monthly Average Time in the Work Queue (as shown in the administrator console) will be less than 1 minute based on a calendar month, provided, that the quantity of email messages above 10MB sent to Cisco Secure Email Cloud Gateway does not exceed 0.01% of all email traffic ("**Delivery Time**"). "**Average Time in the Work Queue**" is the amount of time spent processing a message from the point at which the message is accepted via SMTP to the first SMTP delivery attempt from Cisco Secure Email Cloud Gateway. If You experience a Delivery Time Infraction, then subject to the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Average Delivery Time	Service Credit as a % of Monthly Fee
> 1 minute	20%
> 5 minutes	40%
> 10 minutes	100%

c. Anti-Spam SLA: Cisco Secure Email Cloud Gateway will detect and stop at least 99% of all inbound Spam that is routed through the product. This "**Spam Catch Rate**" is determined by dividing Caught Spam by the sum of the Caught Spam and the number of Missed Spam, during a calendar month. If You experience a Spam Catch Rate Infraction, then subject to the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Spam Catch Rate During Month	Service Credit as a % of Monthly Fee
< 99%	20%
< 98%	40%
<95%	100%

d. False Positive Rate SLA: Cisco Secure Email Cloud Gateway will not categorize legitimate inbound email as Spam more than 1 time per 1 million messages processed. This "**False Positive Rate**" is determined by dividing the number of non-Spam messages misclassified as Spam by the total attempted messages processed during that calendar month.

Exception: This False Positive Rate SLA does not apply to email messages from legitimate senders whose IP addresses may be compromised due to an unforeseen event. We will make a good faith determination based on its system logs, monitoring reports and configuration records for such email senders. In addition, marketing emails with opt-out provisions will not be counted towards the False Positive Rate as those do not constitute Spam as defined in this Offer Description.

Conditions: The False Positive Rate SLA does not apply unless all of the following conditions are met.

- SenderBase reputation filters must be enabled at default levels or more conservatively;
- You must have the reputation messages per connection multiplier set to the default value;
- You must have IronPort Anti-Spam ("**IPAS**") block settings at the default value or more conservatively;
- You must have IPAS quarantine enabled with settings at default or more conservatively;
- You must have SenderBase Network Participation enabled;
- You must provide copies of false positive messages to Us;
- You must provide the domains covered by Cisco Secure Email Cloud Gateway, the number of mailboxes, and the incoming mail report for the last 30 days; and
- You must only enable IPAS for spam scanning to qualify.

If You experience a False Positive Rate Infraction, and subject to the exception and conditions set forth above along with the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

False Positives During a Month	Service Credit as a % of Monthly Fee
> 1 in 1 Million	20%
> 1 in 100 Thousand	40%
> 1 in 1 Thousand	100%

e. Virus Catch Rate SLA: Cisco Secure Email Cloud Gateway will detect and stop 100% of all Known Viruses that are routed through the product within 30 minutes of when the applicable anti-virus provider releases a Virus signature for the platform (the "**Virus Catch Rate**").

Exception: Messages that contain a URL to a website hosting malware and Virus attachments that are password protected are excluded from the Virus Catch Rate.

Conditions: The Virus Catch Rate SLA does not apply unless all of the following conditions are met.

- You must have SenderBase reputation filters enabled at a default level or more aggressively;
- SenderBase Network Participation must be enabled;
- You must provide all samples of missed Viruses to Us;
- You must ensure that the message was scanned by the anti-virus engine (e.g., message did not exceed the maximum scanning size limit); and
- You must provide the domains covered by Cisco Secure Email Cloud Gateway, the number of mailboxes, and the incoming mail report for the last 30 days.

If You experience a Virus Catch Rate Infraction and subject the exception and the conditions set forth above along with the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

Virus Catch Rate During a Month	Service Credit as a % of Monthly Fee
< 100%	20%
< 99%	40%
< 95%	100%

3.5. Cisco Secure Email Encryption Service SLA

Cisco Secure Email Encryption Service will be Operational at least 99.999% of the time during each calendar month, excluding Scheduled Maintenance Windows or Emergency Maintenance. "**Operational**" means that You will have access to Cisco Secure Email Encryption Service for: (1) encrypting emails; (2) enabling secure envelope recipient actions (e.g., opening, secure reply, secure forward, and/or forwarding to mobile@res.cisco.com); and (3) applicable Covered User account access. Cisco Secure Email Encryption Service uptime is determined by dividing the total number of minutes the product was Operational divided by the number of minutes in that calendar month. Each Infraction requires a minimum 30 seconds of downtime.

If You experience a Cisco Secure Email Encryption Service Infraction, subject to the exception above and the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Service Availability	Service Credit as a % of Monthly Fee
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

3.6. Cisco Secure Email Domain Protection and Cisco Secure Email Phishing Defense SLA

We will provide at least 99.999% Service Availability for Cisco Secure Email Domain Protection and Cisco Secure Email Phishing Defense (including but not limited to the portal, hosted sensors (if applicable) and other licensed components) during each calendar month, excluding up to thirty 30 minutes per month for any Scheduled Maintenance Window or Emergency Maintenance.

For the purposes of this section, "**Service Availability**" is determined by the following formula:

(X/Y) x 100 = Service Availability

- "X" = the total number of minutes the applicable Cloud Services is processing messages, and
- "Y" = (the total number of minutes in the calendar month) – (the total number of minutes of downtime from Scheduled Maintenance or Emergency Maintenance which shall not exceed 30 total minutes).

  If the Service Availability is less than 99.999%, and subject to the General Exceptions, We will provide You with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table set forth below.

% of Service Availability per Calendar Month	Service Credit
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

4. Data Protection

4.1. General

Applicable Privacy Data Sheets for the Cloud Services describe the Personal Data that We collect and processes as part of the delivery of the Cloud Services. Additionally, and at Your direction, Cisco Secure Email Cloud Mailbox may send file hashes and/or files submitted to Cisco Secure Email Cloud Mailbox to Cisco Secure Malware Analytics for malware analysis and further threat intelligence research. This only occurs if You choose to turn on the Cisco Secure Malware Analytics integration in Your Cisco Secure Email Cloud Mailbox account. Please see the applicable Privacy Data Sheets available on the Cisco Trust Portal. For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center.

4.2. Cisco Secure Email Domain Protection Data Usage Acknowledgement

We and/or Our applicable subcontractor(s) may use Customer Data relating to emails that fail authentication through Cisco Secure Email Domain Protection ("**Authentication Failure Data**") to provide the Cloud Services and as authorized under the Agreement and this Offer Description. Without limiting rights otherwise set forth in the Agreement and this Offer Description, We (and Our subcontractor(s)) may compile, aggregate, publish, use, and share anonymized summaries of such Authentication Failure Data both during and after the Usage Term to determine and report Cloud Services usage patterns, analyze and report security related issues and trends, and improve upon and create new products and service offerings. You further acknowledge that Us (and Our applicable subcontractor(s) involved in the delivery of the Cloud Services) may license and provide such aggregated and anonymized summary data (excluding Your Confidential Information and any personally identifiable information (if any is actually received)) to Us, Our subcontractors, or their applicable licensees, for internal use in doing the same, both during and after the Usage Term. To the extent You may have any rights in or to any Authentication Failure Data, You hereby grant Us (and Our applicable subcontractor(s) involved in the delivery of the Cloud Services) a perpetual, royalty-free, transferable license to do all of the foregoing. This paragraph will survive the expiration or termination of the Agreement.

5. Support & Maintenance

The Cloud Services include online support and phone support. We will respond as set forth in the tables below and may require information from You to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Us may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. We will respond to a submitted case no later than the next Business Day during Standard Business Hours.

Phone Support provides Cisco Technical Assistance Center ("**TAC**") access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. We will respond within 1 hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, We will respond no later than the next Business Day.

You will also have access to Cisco.com, which provides helpful technical and general information about Our products, as well as access to Our on-line knowledge base and forums. Please note that access restrictions may apply.

The below table outlines Our response objectives based on case severity for the Cisco Secure Email Cloud Gateway, Cisco Secure Email Encryption Service, Cisco Secure Email Phishing Defense, and Cisco Secure Email Domain Protection. We may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic with Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day
Basic with Online Support	Web	Response to all cases within next Business Day during Standard Business Hours	

The below table outlines Our response objectives based on case severity for the Cisco Secure Email Cloud Mailbox. We may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Enhanced	24x7 via Phone & Web	Response within 30 minutes	Response within 2 hours

The following definitions apply to this Section.

"**Response time**" means the time between case submission in the case management system to support engineer contact.

"**Severity 1**" means the Cloud Service is unavailable or down or there is a critical impact to a significant impact to Case Submitter's business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

"**Severity 2**" means the Cloud Service is degraded or significant aspects of Case Submitter's business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

"**Severity 3**" means the Cloud Service is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

"**Severity 4**" means minor intermittent functionality or performance issue, or information is required on the Cloud Service. There is little or no impact to Case Submitter's business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

"**Business Day**" means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

"**Local Time**" means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

"**Standard Business Hours**" means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.